EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	88	726/25	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/26 17:12
S2	1	(test$3 with (strength weakness) with (cipher cryptographic)).ab.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/24 17:20
S3	10	(evaluat$3 with (strength weakness) with (cipher cryptographic)).ab.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/24 17:27
S4	14	(evaluat$3 with (strength weakness) with (key)).ab.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/24 18:21
S5	75	(380/1).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/05/24 18:21
S6	140	(380/2).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/05/24 18:21
S7	1	("7079648").PN.	US-PGPUB; USPAT	OR	OFF	2007/05/26 18:26
S8	1	("6397330").PN.	US-PGPUB; USPAT	OR	OFF	2007/05/26 18:27
S9	4	("6397330").URPN.	USPAT	OR	ON	2007/05/26 18:30
S10	5	("5412717" \| "5651068" \| "5740248" \| "5841869" \| "5907620").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/05/26 18:31
S11	4	("6397330").URPN.	USPAT	OR	ON	2007/05/26 18:35
S12	965	(717/124).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/05/26 18:35
S13	18	S12 and (cryptograph$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/26 18:36

EAST Search History

S14	54	S12 and (cryptograph$2 encrypt$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/26 18:36
S15	2	("5689565" \| "6397330").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/05/26 18:46
S16	4	("6397330").URPN.	USPAT	OR	ON	2007/05/26 18:51
S17	116	(test$3 verif$7 validat$3) near5 (cryptographic near2 (provider (module device facilit$3 component unit card hardware)))	USPAT	OR	ON	2007/05/26 18:55
S18	2777	((717/124-127) or (717/130-135)).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/05/26 18:54
S19	9	S18 and (cryptograph$2 near2 (provider (module device facilit$3 component unit card hardware)))	US-PGPUB; USPAT	OR	ON	2007/05/26 18:55
S20	0	("7079648").URPN.	USPAT	OR	ON	2007/05/26 18:58
S21	0	(cryptograph$2 encryption) near3 correctness near2 detection	USPAT	OR	ON	2007/05/26 18:58
S22	12	(cryptograph$2 encryption) near3 correctness	USPAT	OR	ON	2007/05/26 18:58
S23	19	(cryptograph$2 encryption) near3 correctness	US-PGPUB; USPAT	OR	ON	2007/05/26 19:00
S24	321	(cryptograph$2 encryption) and (acceptable valid proper adequate sufficient satisfactory passable tolerable) near4 (key adj (length size))	US-PGPUB; USPAT	OR	ON	2007/05/26 19:02
S25	24	(cryptograph$2 encryption) and (acceptable valid proper adequate sufficient satisfactory passable tolerable) near4 (key adj (length size)) same (test$3 analy$3 check$3 confirm$5 prov$3 compar$3)	US-PGPUB; USPAT	OR	ON	2007/05/26 19:24
S26	24	(cryptograph$2 encryption) and (acceptable valid proper adequate sufficient satisfactory passable tolerable) near4 (key adj (length size)) same (test$3 analy$3 check$3 confirm$5 prov$3 compar$3 identif$3)	US-PGPUB; USPAT	OR	ON	2007/05/26 19:04

EAST Search History

S27	25	(cryptograph$2 encryption) and (acceptable valid proper adequate sufficient satisfactory passable tolerable) near4 (key adj (length size)) same (test$3 analy$3 check$3 confirm$5 prov$3 compar$3 identification)	US-PGPUB; USPAT	OR	ON	2007/05/26 19:05
S28	214	(cryptograph$2 encryption) near3 (algorithm formula) near3 identifier	US-PGPUB; USPAT	OR	ON	2007/05/26 19:07
S29	622	(cryptograph$2 encryption) near3 (algorithm formula) near3 (parameter identifier)	US-PGPUB; USPAT	OR	ON	2007/05/26 19:07
S30	332	(cryptograph$2 encrypt$3).ab. and ((cryptograph$2 encryption) near3 (algorithm formula) near3 (parameter identifier))	US-PGPUB; USPAT	OR	ON	2007/05/26 19:22
S31	9	("5115466" \| "5412717" \| "5651068" \| "5740248" \| "5778071" \| "5841869" \| "5907620" \| "5933503" \| "6389534").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/05/26 19:19
S32	0	("7013390").URPN.	USPAT	OR	ON	2007/05/26 19:21
S33	4	("6397330").URPN.	USPAT	OR	ON	2007/05/26 19:21
S34	7	("6389534").URPN.	USPAT	OR	ON	2007/05/26 19:21
S35	5	("5412717" \| "5651068" \| "5740248" \| "5841869" \| "5907620").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/05/26 19:21
S36	1	((cryptograph$2 encryption) near3 (algorithm formula) near3 (parameter identifier)) with threshold	US-PGPUB; USPAT	OR	ON	2007/05/26 19:23
S37	1	((cryptograph$2 encryption) near3 (algorithm formula)) with (unacceptable) with acceptable	US-PGPUB; USPAT	OR	ON	2007/05/26 19:24
S38	1	(cryptograph$2 encryption) same (algorithm formula) with (unacceptable) with acceptable	US-PGPUB; USPAT	OR	ON	2007/05/26 19:24
S39	1	(cryptograph$2 encryption) and (acceptable valid proper adequate sufficient satisfactory passable tolerable) near4 (seed adj (length size)) same (test$3 analy$3 check$3 confirm$5 prov$3 compar$3)	US-PGPUB; USPAT	OR	ON	2007/05/26 19:24
S40	1	("20050235342").PN.	US-PGPUB; USPAT	OR	OFF	2007/05/26 22:24

EAST Search History

S41	14	seed near3 (size length) same (algorithm cipher formula encryption cryptographic) same strength	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/26 22:33
S42	83	(test$3 determin$3 compar$3) with seed near3 (size length) same (algorithm cipher formula encryption cryptographic)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/26 22:34
S43	84	(test$3 determin$3 compar$3 evaluat$3) with seed near3 (size length) same (algorithm cipher formula encryption cryptographic)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/05/26 22:34

PORTAL
USPTO
Subscribe (Full Service) Register (Limited Service, Free) Login
Search: The ACM Digital Library The Guide
+cryptographic +test +strength "cryptographic key" "encryptic
SEARCH
THE ACM DIGITAL LIBRARY
Feedback Report a problem Satisfaction survey

Terms used **cryptographic test strength cryptographic key encryption key**

Found **371** of **201,798**

Sort results by relevance
Display results expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next
Best 200 shown Relevance scale

1 Cryptography and data security
Dorothy Elizabeth Robling Denning
January 1982 Book
Publisher: Addison-Wesley Longman Publishing Co., Inc.
Full text available: pdf(19.47 MB) Additional Information: full citation, abstract, references, citings, index terms

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

2 Multiagent systems and electronic markets track: Practical secrecy-preserving, verifiably correct and trustworthy auctions
D. C. Parkes, M. O. Rabin, S. M. Shieber, C. A. Thorpe
August 2006 **Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet ICEC '06**
Publisher: ACM Press
Full text available: pdf(507.45 KB) Additional Information: full citation, abstract, references

We present a practical system for conducting sealed-bid auctions that preserves the secrecy of the bids while providing for verifiable correctness and trustworthiness of the auction. The auctioneer must accept all bids submitted and follow the published rules of the auction. No party receives any useful information about bids before the auction closes and no bidder is able to change or repudiate her bid. Our solution uses Paillier's homomorphic encryption scheme [25] for zero knowledge proofs of ...

3 Public-key cryptography and password protocols
Shai Halevi, Hugo Krawczyk
August 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2

Issue 3
Publisher: ACM Press

Full text available: pdf(275.84 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We study protocols for strong authentication and key exchange in asymmetric scenarios where the authentication server possesses ~a pair of private and public keys while the client has only a weak human-memorizable password as its authentication key. We present and analyze several simple password authentication protocols in this scenario, and show that the security of these protocols can be formally proven based on standard cryptographic assumptions. Remarkably, our analysis shows optimal re ...

Keywords: dictionary attacks, hand-held certificates, key exchange, passwords, public passwords, public-key protocols

4 Approaches to cryptographic key management

Paul G. Comba
September 1986 **Proceedings of the Northeast ACM symposium on Personal computer security PCS '86**
Publisher: ACM Press
Full text available: pdf(680.20 KB) Additional Information: full citation, index terms

5 A security architecture for fault-tolerant systems

Michael K. Reiter, Kenneth P. Birman, Robbert van Renesse
November 1994 **ACM Transactions on Computer Systems (TOCS)**, Volume 12 Issue 4
Publisher: ACM Press

Full text available: pdf(2.50 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Process groups are a common abstraction for fault-tolerant computing in distributed systems. We present a security architecture that extends the process group into a security abstraction. Integral parts of this architecture are services that securely and fault tolerantly support cryptographic key distribution. Using replication only when necessary, and introducing novel replication techniques when it was necessary, we have constructed these services both to be easily defensible against atta ...

Keywords: key distribution, multicast, process groups

6 Survey and benchmark of block ciphers for wireless sensor networks

Yee Wei Law, Jeroen Doumen, Pieter Hartel
February 2006 **ACM Transactions on Sensor Networks (TOSN)**, Volume 2 Issue 1
Publisher: ACM Press

Full text available: pdf(354.39 KB) Additional Information: full citation, appendices and supplements, abstract, references, index terms

Cryptographic algorithms play an important role in the security architecture of wireless sensor networks (WSNs). Choosing the most storage- and energy-efficient block cipher is essential, due to the facts that these networks are meant to operate without human intervention for a long period of time with little energy supply, and that available storage is scarce on these sensor nodes. However, to our knowledge, no systematic work has been done in this area so far. We construct an evaluation framew ...

Keywords: Sensor networks, block ciphers, cryptography, energy efficiency

7 Workshop on architectural support for security and anti-virus (WASSA): Towards the issues in architectural support for protection of software execution

Weidong Shi, Hsien-Hsin S. Lee, Chenghuai Lu, Mrinmoy Ghosh
March 2005 **ACM SIGARCH Computer Architecture News**, Volume 33 Issue 1
Publisher: ACM Press
Full text available: pdf(436.30 KB) Additional Information: full citation, abstract, references, index terms

Recently, there is a growing interest in the research community to employ tamper-resistant processors for software protection. Many of these proposed systems rely on a specially tailored secure processor to prevent 1) illegal software duplication, 2) unauthorized software modification, and 3) unauthorized software reverse engineering. Most of these works primarily focus on the feasibility demonstration and design details rather than trying to elucidate many fundamental issues that are either "el ...

Keywords: attack, copy protection, encryption, security, tamper resistance

8 A model to order the encryption algorithms according to their quality

A. R. Prieto, J. G. Tomas
July 1987 **ACM SIGCOMM Computer Communication Review**, Volume 17 Issue 3
Publisher: ACM Press
Full text available: pdf(565.17 KB) Additional Information: full citation, abstract, index terms

Usually the unicity distance is used to give the strength of encryption algorithms. In this work, the behaviour of encipherment algorithm has been analyzed and two different parameters are proposed in order to evaluate the quality. These parameters are checked against the unicity distance and a final test has been executed, using DES.

9 Security: SECA: security-enhanced communication architecture

Joel Coburn, Srivaths Ravi, Anand Raghunathan, Srimat Chakradhar
September 2005 **Proceedings of the 2005 international conference on Compilers, architectures and synthesis for embedded systems CASES '05**
Publisher: ACM Press
Full text available: pdf(396.53 KB) Additional Information: full citation, abstract, references, index terms

In this work, we propose and investigate the idea of enhancing a System-on-Chip (SoC) communication architecture (the fabric that integrates system components and carries the communication traffic between them) to facilitate higher security. We observe that a wide range of common security attacks are manifested as abnormalities in the system-level communication traffic. Therefore, the communication architecture, with its global system-level visibility, can be used to detect them. The communicati ...

Keywords: AMBA Bus, access control, architecture, attacks, bus, communication, digital rights management (DRM), intrusion detection, security, security-aware design, small embedded systems, system-on-chip (SoC)

10 A new paradigm hidden in steganography

Ira S. Moskowitz, Garth E. Longdon, LiWu Chang
February 2001 **Proceedings of the 2000 workshop on New security paradigms NSPW '00**
Publisher: ACM Press
Full text available: pdf(1.05 MB) Additional Information: full citation, references, citings, index terms

Keywords: information hiding, steganography

11 Strength of two data encryption standard implementations under timing attacks

Alejandro Hevia, Marcos Kiwi
November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4
Publisher: ACM Press

Full text available: pdf(183.73 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We study the vulnerability of two implementations of the Data Encryption Standard (DES) cryptosystem under a timing attack. A timing attack is a method, recently proposed by Paul Kocher, that is designed to break cryptographic systems. It exploits the engineering aspects involved in the implementation of cryptosystems and might succeed even against cryptosys-tems that remain impervious to sophisticated cryptanalytic techniques. A timing attack is, essentially, a way of obtaining some users ...

Keywords: cryptanalysis, cryptography, data encryption standard, timing attack

12 Automatic testing equivalence verification of spi calculus specifications

Luca Durante, Riccardo Sisto, Adriano Valenzano
April 2003 **ACM Transactions on Software Engineering and Methodology (TOSEM)**, Volume 12 Issue 2
Publisher: ACM Press
Full text available: pdf(829.73 KB) Additional Information: full citation, abstract, references, index terms

Testing equivalence is a powerful means for expressing the security properties of cryptographic protocols, but its formal verification is a difficult task because of the quantification over contexts on which it is based. Previous articles have provided insights into using theorem-proving for the verification of testing equivalence of spi calculus specifications. This article addresses the same verification problem, but uses a state exploration approach. The verification technique is based on the ...

Keywords: Cryptographic protocols, equivalence verification, state space exploration

13 Access Control Models and Mechanisms: Cryptographic access control in a distributed file system

Anthony Harrington, Christian Jensen
June 2003 **Proceedings of the eighth ACM symposium on Access control models and technologies SACMAT '03**
Publisher: ACM Press

Full text available: pdf(249.24 KB) Additional Information: full citation, abstract, references, citings, index terms

Traditional access control mechanisms rely on a reference monitor to mediate access to protected resources. Reference monitors are inherently centralized and existing attempts to distribute the functionality of the reference monitor suffer from problems of scalability.Cryptographic access control is a new distributed access control paradigm designed for a global federation of information systems. It defines an implicit access control mechanism, which relies exclusively on cryptography to provide ...

Keywords: access control, cryptography, network file systems

14

Secure and security systems: Satisfiability-based framework for enabling side-channel attacks on cryptographic software

Nachiketh R. Potlapally, Anand Raghunathan, Srivaths Ravi, Niraj K. Jha, Ruby B. Lee

March 2006 **Proceedings of the conference on Design, automation and test in Europe: Designers' forum DATE '06**

Publisher: European Design and Automation Association

Full text available: pdf(161.25 KB) Additional Information: full citation, abstract, references

Many electronic systems contain implementations of cryptographic algorithms in order to provide security. It is well known that cryptographic algorithms, irrespective of their theoretical strength, can be broken through weaknesses in their implementation. In particular, side-channel attacks, which exploit unintended information leakage from the implementation, have been established as a powerful way of attacking cryptographic systems. All side-channel attacks can be viewed as consisting of two p ...

15 Security: Key-assignment strategies for CPPM

André Adelsbach, Jörg Schwenk

September 2004 **Proceedings of the 2004 workshop on Multimedia and security MM&Sec '04**

Publisher: ACM Press

Full text available: pdf(454.53 KB) Additional Information: full citation, abstract, references, index terms

CSS, the first system to protect multimedia content on the new DVD medium failed badly, because both its encryption algorithm and its key management could easily be broken. A new industry initiative, the 4C Entity, LLC (founded by IBM, Intel, Matsushita and Toshiba), presents a more mature approach, called "Copy Protection for Prerecorded Media" (CPPM), which has already been adopted in DVD-Audio.A key-feature of CPPM is its advanced key-management, which allows for system renewability by revoki ...

Keywords: CPPM, content protection, device revocation, key-assignment, key-management

16 Improved proxy re-encryption schemes with applications to secure distributed storage

Giuseppe Ateniese, Kevin Fu, Matthew Green, Susan Hohenberger

February 2006 **ACM Transactions on Information and System Security (TISSEC)**, Volume 9 Issue 1

Publisher: ACM Press

Full text available: pdf(331.59 KB) Additional Information: full citation, abstract, references, index terms

In 1998, Blaze, Bleumer, and Strauss (BBS) proposed an application called *atomic proxy re-encryption*, in which a semitrusted proxy converts a ciphertext for Alice into a ciphertext for Bob *without* seeing the underlying plaintext. We predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. ...

Keywords: Proxy re-encryption, bilinear maps, double decryption, key translation

17 Requirements analysis: Secure systems development based on the common criteria: the PalME project

Monika Vetterling, Guido Wimmel, Alexander Wisspeintner

November 2002 **Proceedings of the 10th ACM SIGSOFT symposium on Foundations of software engineering SIGSOFT '02/FSE-10**

Publisher: ACM Press

Additional Information: full citation, abstract, references, citings, index

Full text available: pdf(640.02 KB) terms

Security is a very important issue in information processing, especially in open network environments like the Internet. The Common Criteria (CC)is the standard requirements catalogue for the evaluation of security critical systems. Using the CC, a large number of security requirements on the system itself and on the system development can be defined. However, the CC does not give methodological support. In this paper, we show how integrate security aspects into the software engineering process. ...

Keywords: AutoFocus, CASE, case study, common criteria, development process, formal methods, graphical description techniques, requirements engineering, security engineering, software design, software engineering

18 Link and channel measurement: A simple mechanism for capturing and replaying wireless channels

Glenn Judd, Peter Steenkiste

August 2005 **Proceeding of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis E-WIND '05**

Publisher: ACM Press

Full text available: pdf(6.06 MB) Additional Information: full citation, abstract, references, index terms

Physical layer wireless network emulation has the potential to be a powerful experimental tool. An important challenge in physical emulation, and traditional simulation, is to accurately model the wireless channel. In this paper we examine the possibility of using on-card signal strength measurements to capture wireless channel traces. A key advantage of this approach is the simplicity and ubiquity with which these measurements can be obtained since virtually all wireless devices provide the req ...

Keywords: channel capture, emulation, wireless

19 Cryptographic sealing for information secrecy and authentication

David K. Gifford

April 1982 **Communications of the ACM**, Volume 25 Issue 4

Publisher: ACM Press

Full text available: pdf(1.29 MB) Additional Information: full citation, abstract, references, citings, index terms

A new protection mechanism is described that provides general primitives for protection and authentication. The mechanism is based on the idea of sealing an object with a key. Sealed objects are self-authenticating, and in the absence of an appropriate set of keys, only provide information about the size of their contents. New keys can be freely created at any time, and keys can also be derived from existing keys with operators that include Key-And and Key-Or

Keywords: conentional crypto-systems, cryptographic sealing, key, seal, secrecy, unseal

20 Security as a new dimension in embedded system design: Security as a new dimension in embedded system design

Srivaths Ravi, Paul Kocher, Ruby Lee, Gary McGraw, Anand Raghunathan

June 2004 **Proceedings of the 41st annual conference on Design automation DAC '04**

Publisher: ACM Press

Full text available: pdf(209.10 KB) Additional Information: full citation, abstract, references, citings, index terms

The growing number of instances of breaches in information security in the last few years

has created a compelling case for efforts towards secure electronic systems. Embedded systems, which will be ubiquitously used to capture, store, manipulate, and access data of a sensitive nature, pose several unique and interesting security challenges. Security has been the subject of intensive research in the areas of cryptography, computing, and networking. However, despite these efforts, *security is ...*

Keywords: *PDAs, architectures, battery life, cryptography, design, design methodologies, digital rights management, embedded systems, performance, security, security processing, security protocols, sensors, software attacks, tamper resistance, trusted computing, viruses*

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player